

# A Near-Optimal Algorithm for Computing Real Roots of Sparse Polynomials

Michael Sagraloff  
Max-Planck-Institut für Informatik, Germany

## ABSTRACT

Let  $p \in \mathbb{Z}[x]$  be an arbitrary polynomial of degree  $n$  with  $k$  non-zero integer coefficients of absolute value less than  $2^\tau$ . In this paper, we answer the open question whether the real roots of  $p$  can be computed with a number of arithmetic operations over the rational numbers that is polynomial in the input size of the sparse representation of  $p$ . More precisely, we give a deterministic, complete, and certified algorithm that determines isolating intervals for all real roots of  $p$  with  $O(k^3 \cdot \log(n\tau) \cdot \log n)$  many exact arithmetic operations over the rational numbers.

When using approximate but certified arithmetic, the bit complexity of our algorithm is bounded by  $\tilde{O}(k^4 \cdot n\tau)$ , where  $\tilde{O}(\cdot)$  means that we ignore logarithmic factors. Hence, for sufficiently sparse polynomials (i.e.  $k = O(\log^c(n\tau))$  for a positive constant  $c$ ), the bit complexity is  $\tilde{O}(n\tau)$ . We also prove that the latter bound is optimal up to logarithmic factors.

## 1. INTRODUCTION

Throughout the following considerations, let

$$p(x) := \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x], \text{ with } |a_i| < 2^\tau \text{ and } \tau \in \mathbb{N}_{\geq 1}, \quad (1.1)$$

be a (not necessarily square-free) polynomial of degree  $n$  with integer coefficients of bit-size less than  $\tau$ , and let  $k$  be the number of non-zero coefficients  $a_{i_0}, \dots, a_{i_{k-1}}$ , with  $0 \leq i_0 < \dots < i_{k-1} = n$ . For convenience, we denote a polynomial  $p \in \mathbb{Z}[x]$  of degree at most  $n$  and with at most  $k$  non-vanishing coefficients, each of absolute value less than  $2^\tau$ , a *k-nomial of magnitude*  $(n, \tau)$ . We assume that  $p$  is given by its sparse representation

$$p(x) = \sum_{l=0}^{k-1} a_{i_l} x^{i_l}, \quad \text{where } a_{i_l} \neq 0 \text{ for all } l = 0, \dots, k-1. \quad (1.2)$$

Notice that the sparse representation needs  $O(k \cdot (\tau + \log n + 1))$  many bits. Namely, we need one bit for the sign of each coefficient  $a_{i_l}$ ,  $\tau$  or less bits for the binary representation of  $|a_{i_l}|$ , and  $\log n$  bits for the binary representation of each index  $i_l$ . To date, it was unknown whether we can isolate (or just count) the real roots of  $p$  with a number of arithmetic operations over  $\mathbb{Q}$  that is polynomial in the input size of the sparse representation of  $p$ . This paper gives a positive answer to the latter question. In addition, we show that, for isolating all real roots of a sparse enough polynomial  $p \in \mathbb{Z}[x]$ , our algorithm is near-optimal:

**THEOREM 1.** *Let  $p \in \mathbb{Z}[x]$  be a  $k$ -nomial of magnitude  $(n, \tau)$ , then we can isolate all real roots of  $p$  with  $O(k^3 \cdot \log(n\tau) \cdot \log n)$  many arithmetic operations over the rational numbers. In addition, for  $k = O(\log^c(n\tau))$ , with  $c$  a non-negative constant, we need at*

*most  $\tilde{O}(n\tau)$  bit operations to isolate all real roots of  $p$ . The latter bound is optimal up to logarithmic factors in  $n$  and  $\tau$ .*

There exist numerous algorithms,<sup>1</sup> e.g. [3, 8, 9, 13, 14, 17, 19, 20, 21, 22, 23, 24], for efficiently computing the real (complex) roots of a polynomial  $p$  as in (1.2), given that  $k$  is large enough. That is, for  $k = \Omega(n^c)$  with  $c$  an arbitrary but positive constant, the computational complexity of these algorithms is polynomial in the input size. For isolating all complex roots of  $p$ , Pan's method [14, 17], which goes back to Schönhage's splitting circle approach [23], achieves record bounds with respect to arithmetic and bit complexity in the worst case. More specifically, it needs  $\tilde{O}(n)$  arithmetic operations performed with a precision of  $\tilde{O}(n\tau)$  bits, and thus,  $\tilde{O}(n^2\tau)$  bit operations. Besides Pan's method, which computes all complex roots at once, there also exist very efficient methods for computing the real roots only. A recently proposed algorithm, denoted ANEWDSC [21], which combines Descartes' Rule of Signs, Newton iteration, and approximate arithmetic, has a bit complexity that is comparable to Pan's method; for any given positive integer  $L$ , ANEWDSC uses  $\tilde{O}(n^3 + n^2\tau + nL)$  bit operations to compute isolating intervals of size less than  $2^{-L}$  for all real roots of  $p$ . We further remark that both of the above mentioned methods can be used to efficiently isolate the roots of a polynomial  $p$  whose coefficients can only be learned from (arbitrarily good) approximations, given that  $p$  has no multiple roots. In this model, the bound on the bit complexity is stated in terms of the degree, the discriminant, and the Mahler bound of  $p$ .

In contrast, for general  $k$ , much less is known about the computational complexity of computing (or just counting) the real roots of  $p$ . In [6], Cucker et al. proposed a method to compute all *integer* roots of  $p$  with a number of bit operations that is polynomial in the input size. Lenstra [10] further showed that all rational roots of  $p$  can be computed in polynomial time. In fact, he even proved that one can compute all factors of  $p$  over  $\mathbb{Q}$  of a fixed degree  $d$  with a number of bit operations that is polynomial in the input size and  $d$ . For trinomials  $p$  (i.e.  $k = 3$ ) with arbitrary real coefficients, Rojas and Ye [18] gave an algorithm for counting (and  $\varepsilon$ -approximating) all real roots of  $p$  that uses  $O(\log^2 n)$  arithmetic operations in the field over  $\mathbb{Q}$  generated by the coefficients of  $p$ . However, already for polynomials  $p \in \mathbb{R}[x]$  with more than 3 monomials, it is unknown whether there exists a deterministic polynomial-time algorithm for computing (or just counting) the real roots of  $p$ . Bastani et al. [1] introduced a deterministic algorithm that, for most inputs, counts the number of real roots of a tetranomial  $p$  (i.e.  $k = 4$ ). Its arithmetic complexity is polynomial in the input size, and, in the special case where  $p$  has integer coefficients, even the bit complexity is polynomial. For general  $k$ -nomials  $p \in \mathbb{Z}[x]$  with integer coefficients, we

<sup>1</sup>The literature on root solving is extensive. Hence, due to space limitations, we decided to restrict to a small selection of representative papers and refer the reader to the references given therein.

are not aware of any method, either for counting or isolating the real roots, that achieves an arithmetic complexity that is polynomial in the input size of the sparse representation of  $p$ .

For the bit complexity, the best known bound for isolating the roots of a (not necessarily sparse polynomial)  $p \in \mathbb{Z}[x]$  is  $\tilde{O}(n^2\tau)$ , and we expect no improvement of the corresponding algorithms when restricting to sparse polynomials. Namely, since Pan's method computes all complex roots, it needs  $\Omega(n)$  arithmetic operations. Also, methods based on Descartes' Rule of Signs need at least  $\Omega(n)$  arithmetic operations due to a transformation of the polynomial  $p$  that destroys its sparsity. This together with the fact that there exist 4-nomials that require a precision of  $\Omega(n\tau)$  for isolating its (real) roots (see also the proof of Theorem 11) indicates that both approaches have a worst-case bit complexity of  $\Omega(n^2\tau)$ . In addition, for isolating the roots of  $p$ , most algorithms need to compute the square-free part of  $p$  in a first step, and the best known deterministic bounds [25, Section 14] for the arithmetic and bit complexity of the latter problem are  $\tilde{O}(n)$  and  $\tilde{O}(n^2\tau)$ , respectively.

Our algorithm is rather simple from a high-level perspective and combines mainly known techniques. Thus, we consider our contribution to be the right assembly of these techniques into an algorithm and the complexity analysis. The main idea underlying our approach is to compute isolating intervals for the roots of  $p_0 := p/x^{i_0}$  from sufficiently small isolating intervals for the roots of the polynomial<sup>2</sup>  $p_1 := p'_0 \cdot x^{1-i_1}$ . Notice that  $p_1$  is a  $(k-1)$ -nomial of magnitude  $(n, \tau + \log n)$  with a non-vanishing constant coefficient. Using evaluation and separation bounds, we can determine the sign of  $p_0$  at the roots of  $p_1$  by evaluating  $p_0$  at arbitrary points in the corresponding isolating intervals, and thus, we can compute common roots of  $p_0$  and  $p_1$ . In addition, we can immediately derive isolating intervals for the simple real roots of  $p_0$  as  $p_0$  is monotone in between two consecutive roots of  $p_1$ . Then, the isolating intervals for the roots of  $p_0$  can be further refined to an arbitrary small size. Hence, recursive application of the above approach allows us to compute isolating intervals for  $p$  from the roots of a 1-nomial  $p_{k-1} \in \mathbb{Z}[x]$  after  $k$  iterations; see Section 2.1 for details.

Efficiency of the above approach crucially depends on the method to refine the isolating intervals for the simple roots of the polynomials  $p_i$  that are considered in the recursion. For this, we modify an efficient method for approximating (clusters of) real roots as recently proposed in [21]. Since the method from [21] is based on Descartes' Rule of Signs, its arithmetic complexity is super-linear in  $n$ . Hence, in order to exploit the sparsity of the polynomials  $p_i$ , we had to replace the corresponding steps by simple polynomial evaluation. For an arbitrary positive integer  $L$ , the so-obtained method refines arbitrarily isolating intervals for all simple roots of a  $k$ -nomial  $p$  of magnitude  $(n, \tau)$  to a size less than  $2^{-L}$  in  $O(k \cdot (\log n + \log(\tau + L)))$  iterations, and, in each iteration,  $p$  is evaluated at a constant number of points. This yields an arithmetic complexity for the refinement steps that is polynomial in the input size. We consider the refinement method as the key ingredient of our algorithm, and think that it is of independent interest.

When using exact arithmetic over the rationals, the bit complexity of our algorithm is  $\tilde{O}(k^3 \cdot n^2\tau)$ . We further show that, when replacing exact by approximate computation, the bit-size of the intermediate results reduces by a factor  $n$  for the price of using  $k$  times as many arithmetic operations. This yields the bound  $\tilde{O}(k^4 \cdot n\tau)$ , and thus,  $\tilde{O}(n\tau)$  for sufficiently small  $k$ , that is,  $k = O(\log^c(n\tau))$ . We also prove that the latter bound is optimal, where we use the fact that

there exist 4-nomials such that the binary representations of the corresponding isolating intervals need  $\Omega(n\tau)$  bits.

## 2. ALGORITHM AND COMPLEXITY

### 2.1 The Algorithm

It is well known (e.g., see [6, 18]) that the number of real roots of  $p$  is upper bounded by  $2k - 1$ . Namely, according to Descartes' Rule of Signs, the number of positive real roots of  $p$  (counted with multiplicity) is upper bounded by the number of sign changes in the coefficient sequence of  $p$ , and thus, smaller than  $k$ . The same argument applied to the polynomial  $p(-x)$  further shows that the number of negative roots of  $p(x)$  is smaller than  $k$  as well.

In what follows, we may assume, w.l.o.g., that  $i_0 = 0$ . Namely, if  $i_0 > 0$ , then  $p$  has the same roots as  $p/x^{i_0}$  plus an additional root at  $x = 0$  of multiplicity  $i_0$ . Hence, we can consider the polynomial  $p/x^{i_0}$  instead. In addition, we may restrict our search to the positive roots; for the negative roots, we can then apply the same approach to the polynomial  $p(-x)$ . According to Cauchy's root bound, the modulus of each (complex) root is upper bounded by  $1 + 2^\tau < 2^{\tau+1}$ , and thus, for isolating the positive real roots of  $f$ , we can restrict our search to the interval  $\mathcal{I} := (0, 2^{\tau+1})$ . We write  $p$  as

$$p(x) = a_{i_0} + x^{i_1} \cdot (a_{i_1} + \dots + a_{i_{k-1}} \cdot x^{i_{k-1}-i_1}) = a_{i_0} + x^{i_1} \cdot \hat{p}(x),$$

where  $\hat{p}$  has degree  $n - i_1 < n$  and exactly  $k - 1$  non-zero coefficients. The idea is now to compute isolating intervals for the positive roots of  $p_0 := p$  from sufficiently small isolating intervals for the positive roots of its derivative  $p'(x) := \frac{dp(x)}{dx}$ . For this, we do not directly consider the derivative  $p'(x)$  but the polynomial

$$p_1(x) := x \cdot \hat{p}'(x) + i_1 \cdot \hat{p}(x) = \frac{p'(x)}{x^{i_1-1}}, \quad (2.1)$$

which has the same roots as  $p'$  except for the root at  $x = 0$  of multiplicity  $i_1 - 1$ . Notice that  $p_1$  is a  $(k-1)$ -nomial of magnitude  $(n - i_1, \tau + \log n)$  and that its coefficients can be computed from the coefficients of  $p$  using  $k$  multiplications and  $k$  additions.

Let  $x'_1$  to  $x'_{k_1}$ , with  $0 \leq k_1 \leq k - 2$ , denote the roots of  $p_1$  that are contained in  $\mathcal{I} = (0, 2^{\tau+1})$ . W.l.o.g., we may assume that  $0 < x'_1 < x'_2 < \dots < x'_{k_1} < 2^{\tau+1}$ . Now, suppose that, for each root  $x'_j$ , an isolating interval  $I'_j = (a_j, b_j) \subset \mathcal{I}$  of width less than  $2^{-L}$ , with  $L := 128 \cdot n \cdot (\tau + k \cdot \log n)$  and  $a_j, b_j \in \mathbb{Q}$ , is given. Then, based on the following theorem, we can compute the sign of  $p$  at the roots of  $p_1$ , and thus, determine common roots of  $p$  and  $p_1$ . Because of space limitations, we give the proof of Theorem 2 in the Appendix. It mainly combines known results, however, we remark that we could not find a comparable result in the literature, where only evaluation/separation bounds of size  $\tilde{O}(n^2 + n\mu)$  are given.

**THEOREM 2.** *Let  $f$  and  $g$  be polynomials of degree  $n$  or less with integer coefficients of absolute values less than  $2^\mu$ , and let*

$$L := 128 \cdot n \cdot (\log n + \mu). \quad (2.2)$$

*Then, for any two distinct roots  $\xi_i$  and  $\xi_j$  of  $F := f \cdot g$ , it holds that  $|\xi_i - \xi_j|^{m_i} > 2^{-L}$ , where  $m_i := \text{mult}(\xi_i, F)$  denotes the multiplicity of  $\xi_i$  as a root of  $F$ . If  $\xi$  is a root of  $g$  and  $f(\xi) \neq 0$ , then it holds that  $|f(x)| > 2^{-L/4}$  for all  $x \in \mathbb{C}$  with  $|x - \xi| < 2^{-L}$ . Vice versa, if  $f(\xi) = 0$ , then  $|f(x)| < 2^{-L}$  for all  $x \in \mathbb{C}$  with  $|x - \xi| < 2^{-L}$ .*

From the above theorem, we conclude that, for all  $j = 1, \dots, k_1$ :

- $p$  has at most one root  $\xi$  in  $I'_j$ .
- If  $p$  has a root  $\xi$  in  $I'_j$ , then  $\xi = x'_j$  and  $|p(x)| < 2^{-L}$  for all  $x \in I'_j$ .
- If  $p$  has no root in  $I'_j$ , then  $|p(x)| > 2^{-L/4}$  for all  $x \in I'_j$ .

<sup>2</sup>For simplicity, the reader may assume that  $i_0 = 0$ , and thus,  $p_1$  has the same roots as the derivative  $p' = \frac{dp}{dx}$  of  $p$  except for the root at zero.

Hence, we can determine the sign of  $p$  at each root  $x'_j$  of  $p_1$  by evaluating  $p(x)$  to an absolute error<sup>3</sup> of less than  $2^{-L/2}$ , where  $x$  is an arbitrary point in  $I'_j$ . Let  $x'_0 := 0$  and  $x'_{k+1} := 2^{\tau+1}$ , and let  $I'_0 = [a_0, b_0] := [x'_0, x'_0]$  and  $I'_{k+1} = [a_{k+1}, b_{k+1}] := [x'_{k+1}, x'_{k+1}]$  be corresponding intervals of width 0. Notice that the values  $x'_j$  decompose  $\mathcal{S}$  into  $k_1 + 1$  many intervals  $A_j := (x'_{j-1}, x'_j)$  such that  $p$  is monotone in each interval  $A_j$ . In addition, if either  $p(x'_{j-1}) = 0$  or  $p(x'_j) = 0$ , then  $p$  has no root in  $A_j$  according to Rolle's Theorem. Hence,  $p$  has a root  $\xi$  in  $A_j$  if and only if  $p(x'_{j-1}) \cdot p(x'_j) < 0$ . If the latter inequality holds, then  $\xi$  is unique and simple. In fact, it even holds that the shortened interval  $A'_j := (a_{j-1}, b_{1,j}) \subset A_j$  isolates  $\xi$  because  $I'_{j-1}$  and  $I'_j$  do not contain any root of  $p$ . Now, since we can compute the sign of  $p$  at all points  $x'_j$ , isolating intervals for the positive real roots of  $p$  can directly be derived from the intervals  $I'_j$ . Notice that, for the positive roots of  $p$  with multiplicity larger than 1, isolating intervals of width less than  $2^{-L}$  are already given. Namely, the multiple roots of  $p$  are exactly the common roots of  $p$  and  $p_1$ , and thus they are already isolated by some of the intervals  $I'_j$ . Each simple positive root of  $p$  is isolated by an interval  $A'_j$ , which can be further refined to a width less than  $2^{-L}$  using the refinement method from Section 3. In summary, we have shown how to compute isolating intervals of width less than  $2^{-L}$  for all roots of  $p$  contained in  $\mathcal{S}$  from isolating intervals of width less than  $2^{-L}$  for all roots of  $p_1$  that are contained in  $\mathcal{S}$ .

We now recursively apply the above approach to  $p_1$ . More explicitly, for  $j = 1, \dots, k-1$ , we first compute the polynomials

$$p_0 := p, \quad p_j := x \cdot \hat{p}'_{j-1} + (i_j - i_{j-1}) \cdot \hat{p}_j = x^{-(i_j - i_{j-1} + 1)} \cdot p'_{j-1}(x),$$

where  $p_{j-1} = p_{j-1}(0) + x^{i_j - i_{j-1}} \cdot \hat{p}_{j-1}(x)$ , and  $\hat{p}_{j-1}(0) \neq 0$ .

Since  $p_j$  is a  $(k-j)$ -nomial of magnitude  $(n - i_j, \tau + j \cdot \log n)$ ,  $p_j$  becomes a constant for  $j = k-1$ . Thus, computing isolating intervals of width less than  $2^{-L}$  for the positive roots of  $p_{k-1}$  is trivial. Going backwards from  $j = k-1$ , we can then iteratively compute isolating intervals  $I_{j-1,1}$  to  $I_{j-1,k_j}$  of width less than  $2^{-L}$  for the roots of  $p_{j-1}$  from isolating intervals  $I_{j,1}$  to  $I_{j,k_j}$  of width less than  $2^{-L}$  for the roots of  $p_j$ . Notice that Theorem 2 applies to  $f := p_{j-1}$ ,  $g := p_j$  and any point  $x \in I_{j,i}$  as  $I_{j,i}$  has width less than  $2^{-L}$  and  $L = 128 \cdot n \cdot (n + k \cdot \log n) \geq 128 \cdot \max(\deg(p_{j-1}), \deg(p_j)) \cdot (\log \max(\|p_{j-1}\|_\infty, \|p_j\|_\infty) + \log n)$  for all  $j \leq k-1$ . Hence, we can compute the sign of  $p_{j-1}$  at each positive root of  $p_j$  by evaluating  $p_{j-1}$  at an arbitrary point in the corresponding isolating interval.

Notice that the above approach does not only yield isolating intervals for all real roots of  $p$  but also the corresponding multiplicities. Namely, a root  $\xi$  of  $p$  has multiplicity  $j$  if and only if  $p_0(\xi) = \dots = p_{j-1}(\xi) = 0 \neq p_j(\xi)$ .

Before we continue with the analysis of our algorithm, we first consider a simple example to illustrate our approach. Notice that we tried to keep the formulation of our algorithm as simple as possible with the prior goal to achieve the claimed complexity bounds, however, for the cost of a probably worse performance in practice. Hence, for an actual implementation, we propose to integrate additional steps in order to avoid costly refinement steps, and thus, to considerably speed up the overall approach. We hint to such techniques in the following section. The reader who is mainly interested in the theoretical complexity bounds should feel free to skip the

example and directly continue with Section 2.3.

## 2.2 An Example and Alternatives

Let  $p(x) = x^{50} - 4 \cdot x^{48} + 4 \cdot x^{46} - x^4 + 4 \cdot x^2 - 4$  be a 6-nomial of magnitude  $(n, \tau) := (50, 2)$ . We consider the polynomials  $p_j$ , with  $j = 0, \dots, 5$ , that are defined as follows:

$$\begin{aligned} p_0(x) &:= x^{50} - 4 \cdot x^{48} + 4 \cdot x^{46} - x^4 + 4 \cdot x^2 - 4 \\ &= x^2 \cdot (x^{48} - 4 \cdot x^{46} + 4 \cdot x^{44} - x^2 + 4) - 4 = x^2 \cdot \hat{p}_0 - 4 \\ p_1(x) &:= x \cdot \hat{p}'_0 + 2 \cdot \hat{p}_0 = x^{-1} \cdot p'_0(x) = \\ &= x^2 \cdot (50 \cdot x^{46} - 192 \cdot x^{44} + 184 \cdot x^{42} - 4) + 8 = x^2 \cdot \hat{p}_1 + 8 \\ p_2(x) &:= x \cdot \hat{p}'_1 + 2 \cdot \hat{p}_1 = x^{-1} \cdot p'_1(x) = \\ &= x^{42} \cdot (2400 \cdot x^4 - 8832 \cdot x^2 + 8096) - 8 = x^{42} \cdot \hat{p}_2 - 8 \\ p_3(x) &:= x \cdot \hat{p}'_2 + 42 \cdot \hat{p}_2 = x^{-41} \cdot p'_2(x) = \\ &= x^2 \cdot (110400 \cdot x^2 - 388608) + 340032 = x^2 \cdot \hat{p}_3 + 340032 \\ p_4(x) &:= x \cdot \hat{p}'_3 + 2 \cdot \hat{p}_3 = x^{-1} \cdot p'_3(x) = \\ &= x^2 \cdot 441600 - 777216 = x^2 \cdot \hat{p}_4 - 777216 \\ p_5(x) &:= x \cdot \hat{p}'_4 + 2 \cdot \hat{p}_4 = x^{-1} \cdot p'_4(x) = 883200 \end{aligned}$$

We want to recursively isolate and approximate the positive real roots of the polynomials  $p_5$  to  $p_0$ , starting with  $p_5$ . Since we are only interested in the roots of  $p = p_0$ , we can restrict to the interval  $\mathcal{S} := (0, 8)$ , which must contain all positive roots of  $p$ . Trivially,  $p_5$  has no root, and thus,  $p_4$  is monotone in  $\mathcal{S}$ . Since  $p_4(0) < 0$  and  $p_4(8) > 0$ , the interval  $I_{4,1} := \mathcal{S}$  isolates the unique (simple) positive real root (at  $x_{4,1} \approx 1.326$ ) of  $p_4$  in  $\mathcal{S}$ . The polynomial  $p_3$  is monotone in each of the two intervals  $(0, x_{4,1})$  and  $(x_{4,1}, 8)$ . Refining the isolating interval for  $x_{4,1}$  to a width less than  $2^{-L}$ , with  $L := 128 \cdot \deg(p) \cdot (\log \|p\|_\infty + 6 \cdot \log \deg(p)) \approx 8.5 \cdot 10^4$ , and using Theorem 2, we can evaluate the sign of  $p_3$  at  $x = x_{4,1}$ . Since  $p_3(0) > 0$ ,  $p_3(x_{4,1}) \approx -1943 < 0$ , and  $p_3(8) > 0$ , each of the two intervals  $I_{3,1} := (0, x_{4,1})$  and  $I_{3,2} := (x_{4,1}, 8)$  isolates a (simple) positive real root (at  $x_{3,1} \approx 1.275$  and at  $x_{3,2} \approx 1.375$ ) of  $p_3$ . The polynomial  $p_2$  is monotone in each of the three intervals  $(0, x_{3,1})$ ,  $(x_{3,1}, x_{3,2})$ , and  $(x_{3,2}, 8)$ . We again refine the isolating intervals for  $x_{3,1}$  and  $x_{3,2}$  to a width less than  $2^{-L}$  and evaluate the sign of  $p_2$  at the points  $x = 0$ ,  $x = 8$ , and at the roots of  $p_3$ . From the latter evaluations, we conclude that  $p_2$  has exactly three positive (simple) real roots (at  $x_{2,1} := 0.869 \dots$ ,  $x_{2,2} \approx 1.315$ , and at  $x_{2,3} \approx 1.396$ ), which are isolated by the intervals  $I_{2,1} := (0, x_{3,1})$ ,  $I_{2,2} := (x_{3,1}, x_{3,2})$ , and  $I_{2,3} := (x_{3,2}, 8)$ , respectively. Refining the isolating intervals for  $x_{2,1}$ ,  $x_{2,2}$ , and  $x_{2,3}$  to a width less than  $2^{-L}$  again allows us to evaluate the sign of  $p_1$  at the roots of  $p_2$ . The latter computation shows that  $p_1$  has exactly two (simple) positive real roots in  $\mathcal{S}$  (at  $x_{1,1} \approx 1.356$  and at  $x_{1,2} \approx 1.414$ ), which are isolated by the intervals  $(x_{2,2}, x_{2,3})$  and  $(x_{2,3}, 8)$ , respectively. Eventually, we refine the intervals to a width less than  $2^{-L}$  and evaluate the sign of  $p_0 = p$  at the roots of  $p_1$ . We have  $p_0(x_{1,1}) \approx 3 \cdot 10^4$  and  $p_0(x) < 2^{-L}$ , where  $x$  has been arbitrary chosen from the isolating interval for  $x_{1,2}$ . Hence, from Theorem 2, we conclude that  $p_0(x_{1,2}) = 0$ , and thus,  $x_{0,1} := x_{1,2}$  is the unique positive real root of  $p$ . In addition,  $x_{0,1}$  has multiplicity 2.

Notice that, in each except the last step (i.e. for  $j = 2, \dots, 5$ ), we could consider an alternative approach, where we simultaneously refine the isolating interval for a root  $\xi$  of  $p_j$  and use interval arithmetic to evaluate the sign of  $p_{j-1}(\xi)$ . Following the analysis in [11, Section 4], one can show that, if  $p_{j-1}(\xi) \neq 0$ , then this approach yields the correct sign as soon as the interval has been refined to a width less than  $2^{-L'}$ , with  $L' = \deg(p_{j-1}) \cdot (4 + \log \max(1, |\xi|)) -$

<sup>3</sup>For now, you may assume that we exactly evaluate  $p(x)$  for some rational  $x \in I'_j$ . However, we will need the more general statement for our version of the algorithm that uses approximate arithmetic, as proposed in Section 4.

$\log |p_{j-1}(\xi)| + \tau$ . For instance, in our example above, the sign of  $p_3$  at the root  $x_{4,1}$  of  $p_4$  can be determined from an isolating interval for  $x_{4,1}$  of width less than  $2^{-11}$  (compared to the theoretical bound of approximate size  $2^{-8.5 \cdot 10^4}$  from Theorem 2). Hence, for a practical implementation, we strongly recommend to integrate such techniques to rule out easy cases in a more efficient way. However, for deciding that  $p_0$  evaluates to zero at  $x = x_{1,2}$ , methods that are purely based on approximate computation will not work.<sup>4</sup> One possible way, as proposed in our algorithm, is to refine the isolating interval for  $x_{1,2}$  to a sufficiently small size, to evaluate  $p$  at an arbitrary point that is contained in the isolating interval, and to apply Theorem 2. Another way is to compute the square-free part  $g^*$  of the greatest common divisor  $g := \gcd(p_{j-1}, p_j)$  of  $p_{j-1}$  and  $p_j$  and to check whether  $g^*$  changes signs at the endpoints of the isolating interval. The advantage of the latter approach is that  $p_{j-1}$  and  $p_j$  typically do not share a common non-trivial factor, which can be easily checked via modular computation, and thus, it suffices to use interval arithmetic to compute the sign of  $p_{j-1}$  at the roots of  $p_j$ .

However, although the second approach, which is based on computing  $g^*$ , seems to be more efficient in practice, there is a severe drawback with respect to its arithmetic complexity. Namely, the considered symbolic computations need a number of arithmetic operations that is super-linear in the degree of the involved polynomials. In contrast, we will show that the first approach, which is entirely based on refinement and evaluation, only uses a number of arithmetic operations that is polynomial in the input size of the sparse representation of the input polynomial.

### 2.3 Arithmetic Complexity

For an arbitrary  $k$ -nomial  $p \in \mathbb{Z}[x]$  of magnitude  $(n, \tau)$ , suppose that each simple positive root  $\xi$  of  $p$  is already isolated by a corresponding interval  $I = (a, b) \subset \mathcal{J} = (0, 2^{\tau+1})$  with rational endpoints  $a$  and  $b$ . In Section 3, we give an algorithm to refine *all* such isolating intervals to a width less than  $2^{-L}$  using  $O(k^2 \cdot (\log(n\tau) + \log L) \cdot \log n)$  arithmetic operations over  $\mathbb{Q}$ . Hence, from the definition of our algorithm for root isolation, we conclude that we can compute isolating intervals of width less than  $2^{-L}$ , with  $L := 128 \cdot n \cdot (n + k \cdot \log n)$ , for all roots of  $p_{j-1}$  contained in  $\mathcal{J}$  from isolating intervals of size less than  $2^{-L}$  for the roots of  $p_j$  contained in  $\mathcal{J}$  using only  $O(k^2 \cdot \log(n\tau) \cdot \log n)$  many arithmetic operations: Namely, we can compute  $p_j$  from  $p_{j-1}$  with  $k$  multiplications and  $k$  additions. For evaluating  $p_{j-1}$  at an arbitrary point  $x \in \mathbb{Q}$ , we need at most  $2k \log n$  arithmetic operations since we can compute  $x^i$  with less than  $2 \log i$  multiplications by repeated squaring (e.g.  $x^{11} = x \cdot x^2 \cdot ((x^2)^2)^2$ ) and  $p_{j-1}$  has at most  $k$  non-vanishing coefficients. We have shown that evaluating the sign of  $p_{j-1}$  at each root  $\xi \in \mathcal{J}$  of  $p_j$  can be reduced to the evaluation of  $p_{j-1}$  at an arbitrary (rational) point  $x \in I'$ , where  $I'$  is an isolating interval for  $\xi$ . Hence, the latter evaluations need at most  $(k+1) \cdot (2k \log n)$  many arithmetic operations as each polynomial  $p_j$  is a  $(k-j)$ -nomial of magnitude  $(n - i_j, \tau + j \cdot \log n)$ . Finally, the refinement of the isolating intervals for the simple positive roots of  $p_{j-1}$  needs  $O(k^2 \cdot \log(n\tau) \cdot \log n)$  many arithmetic operations. Hence, the total number of arithmetic operations is bounded by

$$k \cdot (3k + 2k^2 \log n + O(k^2 \cdot \log(n\tau) \cdot \log n)).$$

We fix this result:

<sup>4</sup>That is, without computing an explicit theoretical evaluation bound  $2^{-L}$  as given in Theorem 2. Certainly, if one is willing to use such a bound, then also numerical computation will yield the correct result as soon as the interval has size less than  $2^{-L}$  and the precision of the approximate arithmetic is large enough to guarantee an absolute error of less than  $2^{-L/2}$ .

**THEOREM 3.** *Let  $p \in \mathbb{Z}[x]$  be a  $k$ -nomial of magnitude  $(n, \tau)$ , then all real roots of  $p$  can be isolated with  $O(k^3 \cdot \log(n\tau) \cdot \log n)$  arithmetic operations over the rational numbers.*

Notice that, from the latter theorem, we can immediately derive a corresponding result for polynomials  $p(x) = \sum_{i=0}^{k-1} a_i x^{q_i} \in \mathbb{Q}[x]$  with rational coefficients. Namely, suppose that  $a_i = \frac{p_i}{q_i}$ , with integers  $p_i$  and  $q_i$  of absolute values less than  $2^\tau$ . Then,  $P(x) := p(x) \cdot \prod_{i=0}^{k-1} q_i \in \mathbb{Z}[x]$  is a  $k$ -nomial of magnitude  $(n, k\tau)$  that has the same roots as  $p(x)$ . Since  $P$  can be computed from  $p$  using less than  $2k$  multiplications, we conclude from Theorem 3:

**COROLLARY 4.** *Let  $p(x) = \sum_{i=0}^{k-1} a_i x^{q_i} \in \mathbb{Q}[x]$  be a polynomial with rational coefficients of the form  $a_i = \frac{p_i}{q_i}$ , where  $p_i, q_i \in \mathbb{Z}$  and  $|p_i|, |q_i| < 2^\tau$  for all  $i = 0, \dots, k-1$ . Then, all real roots of  $p$  can be isolated with  $O(k^3 \cdot \log(kn\tau) \cdot \log n)$  arithmetic operations over the rational numbers.*

### 3. ROOT REFINEMENT

Throughout the following considerations, let  $p(x)$  be a  $k$ -nomial of magnitude  $(n, \tau)$  as in (1.1), and let  $I_0 = (a_0, b_0) \subset \mathcal{J} = (0, 2^{\tau+1})$ , with  $a_0, b_0 \in \mathbb{Q}$ , be an isolating interval for a simple real root  $\xi$  of  $p$ . For a given positive integer  $L \in \mathbb{Z}$ , we aim to refine  $I_0$  to a width less than  $2^{-L}$ . Our refinement method is almost identical to a combination of the *Newton-* and the *Boundary-Test* as proposed in a very recent paper [21] on real root isolation, however, we slightly modify the latter approach in order to exploit the sparsity of  $p$ . That is, for testing an interval  $I \subset I_0$  for the existence of a root, we replace a test based on Descartes' Rule of Signs (see Theorem 5) by a simple sign evaluation of  $p$  at the endpoints of  $I$ . For refining  $I_0$ , this is possible as  $I_0$  is assumed to be isolating for a simple root, whereas the method from [21] has to process arbitrary intervals for which no further information is provided.<sup>5</sup>

For the sake of a self-contained presentation, we briefly review some basic facts about Descartes' Rule of Signs before presenting the refinement algorithm; for an extensive treatment of the Descartes method, we refer to [5, 7, 8, 20, 21]:

For an arbitrary interval  $I = (a, b)$ , we denote  $\text{var}(p, I)$  the number of sign variations in the coefficient sequence  $(a_{l,0}, \dots, a_{l,n})$  (after removing all zero-entries) of the polynomial

$$p_I(x) = \sum_{i=0}^n a_{l,i} x^i := (x+1)^n \cdot f\left(\frac{a \cdot x + b}{x+1}\right). \quad (3.1)$$

The polynomial  $p_I$  is computed from  $p$  via the Möbius transformation that maps a point  $x \in \mathbb{C} \setminus \{-1\}$  to  $\frac{a \cdot x + b}{x+1} \in \mathbb{C}$ , followed by multiplication with  $(x+1)^n$ . Notice that the latter step ensures that denominators in  $p((ax+b)/(x+1))$  are cleared. There is a one-to-one correspondence (preserving multiplicities) between the positive real roots of  $p_I$  and the roots of  $p$  in  $I$ . In addition, according to Descartes' Rule of Signs,  $v := \text{var}(p, I)$  is an upper bound on the

<sup>5</sup>The Newton-Test from [21, Section 3.2] is a crucial subroutine within the root isolation algorithm ANEWDESC. It guarantees that, during the isolation process, clusters of roots are automatically detected and further approximated in an efficient manner. In this setting, the Newton-Test applies to arbitrary intervals  $I$  that are not known to be isolating yet. Notice that, for the refinement of  $I_0$ , we cannot directly use the original Newton-Test from [21]. Namely, in general, the polynomial  $p_I$  from (3.1) is not sparse anymore, even for small  $k$ , and thus, we would need a super linear number of arithmetic operations to compute  $\text{var}(p, I)$  (see Thm. 5 for definitions). However, when refining an interval  $I_0$  that is known to isolate a simple real root  $\xi$  of  $p$ , we can test a subinterval  $I \subset I_0$  for being isolating with only two evaluations of  $p$ . Namely,  $I$  isolates  $\xi$  if and only if  $p(a) \cdot p(b) < 0$ .

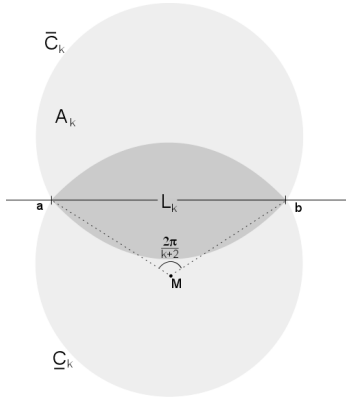


Figure 3.1: For an arbitrary integer  $k \in \{0, \dots, n\}$ , let  $\bar{C}_k$  and  $C_k$  for  $I := (a, b)$  have the endpoints of  $I$  on their boundaries; their centers see the line segment  $ab$  under the angle  $\frac{2\pi}{k+2}$ . The Obreshkoff lens  $L_k$  is the interior of  $\bar{C}_k \cap C_k$ , and the Obreshkoff area  $A_k$  is the interior of  $\bar{C}_k \cup C_k$ .  $A_0$  and  $A_1$  are called the One- and Two-Circle Regions of  $I$ , respectively.

number  $m$  of real roots of  $p$  in  $I$  and  $v - m$  is an even integer. The function  $\text{var}(p, \cdot)$  has several further important properties:

**THEOREM 5.** [7, 15, 16] *Let  $I = (a, b)$  be an arbitrary interval, and let  $L_i$  and  $A_i$ , with  $i = 0, 1, \dots, n$ , be the Obreshkoff regions in  $\mathbb{C}$  as defined in Figure 3.1. Then, it holds that (roots are counted with multiplicity):*

- (a) # roots contained in  $L_n \leq \text{var}(p, I) \leq \#$  roots contained in  $A_n$
- (b) If  $p$  contains no root in  $A_0$ , then  $\text{var}(p, I) = 0$ . If  $A_1$  contains exactly one root, then  $\text{var}(p, I) = 1$ .
- (c) If  $I_1$  and  $I_2$  are two disjoint subintervals of  $I$ , then
$$\text{var}(p, I_1) + \text{var}(p, I_2) \leq \text{var}(p, I).$$

From Theorem 5 (c), we conclude that, for any interval  $I = (a, b) \subset \mathbb{R}_{>0}$  on the positive real axis,  $\text{var}(p, I)$  is upper bounded by  $\text{var}(p, (0, b)) = \text{var}(p)$ , and thus,  $\text{var}(p, I) \leq k - 1$ . In particular, we have  $\text{var}(p, I_0) \leq k - 1$ . Hence, part (a) of Theorem 5 implies that the Obreshkoff lens  $L_n$  of  $I_0$  contains at most  $k - 1$  roots of  $p$ .

We can now formulate our refinement method. As mentioned above, it is almost identical to the approach presented in [21, Section 3.2], hence we keep the presentation as short as possible and refer to the corresponding paper for more explanations and for a discussion that motivates the approach:

The main idea is to iteratively refine  $I_0$  such that, in each iteration, we replace an isolating interval  $I = (a, b) \subset I_0$  by an isolating interval  $I' = (a', b') \subset I$  of considerably smaller width, and with  $a', b' \in \mathbb{Q}$ . For this, we use two main ingredients, namely, sign evaluation of  $p$  at the endpoints of  $I'$  in order to test  $I'$  for the existence of a root, and a subdivision strategy based on Newton iteration and bisection, which guarantees quadratic convergence in the majority of all step. We give details:

#### Algorithm NEWREFINE (read Newton-Refine)

**Input:** An interval  $I_0 = (a_0, b_0) \subset \mathcal{I} = (0, 2^{\tau+1})$ , with endpoints  $a_0, b_0 \in \mathbb{Q}$ , that isolates a simple root  $\xi \in \mathbb{R}$  of a polynomial  $p \in \mathbb{Z}[x]$ , and a positive integer  $L$ .

**Output:** An interval  $I = (a, b) \subset I_0$ , with endpoints  $a, b \in \mathbb{Q}$ , of width less than  $2^{-L}$  that isolates  $\xi$ .

In each step of the recursion, we store a pair  $\mathcal{A} := (I, N_I)$ , where we initially set  $\mathcal{A} := (I_0, N_{I_0})$ , with  $N_{I_0} := 4$ . We first try to compute a subinterval  $I' \subset I$  of width  $w(I')$ , with  $\frac{w(I)}{8N_I} \leq w(I') \leq \frac{w(I)}{N_I}$ , that contains the unique root  $\xi$ . This is done via two tests, that is, the `Newton-Test_signat` and the `Boundary-Test_signat`.<sup>6</sup>

**Newton-Test\_signat:** Consider the points  $\xi_1 := a + \frac{1}{4} \cdot w(I)$ ,  $\xi_2 := a + \frac{1}{2} \cdot w(I)$ ,  $\xi_3 := a + \frac{3}{4} \cdot w(I)$ , and let  $\varepsilon := 2^{-\lceil 5 + \log n \rceil}$ . For  $j = 1, 2, 3$ , we choose arbitrary points (see Footnote 6)

$$\xi_j^* \in \xi_j[\varepsilon \cdot w(I)], \quad (3.2)$$

where, for an arbitrary  $m \in \mathbb{R}$  and an arbitrary  $\delta \in \mathbb{R}_{>0}$ , we define

$$m[\delta] := \{m_i := m + (i - \lfloor k/2 \rfloor) \cdot \delta; i = 0, \dots, 2 \cdot \lfloor k/2 \rfloor\}.$$

The points  $\xi_j^*$  define values  $v_j := \frac{p(\xi_j^*)}{p'(\xi_j^*)}$ . Then, for the three distinct pairs of indices  $i, j \in \{1, 2, 3\}$  with  $i < j$ , we perform the following computations in parallel: For  $L = 1, 2, 4, \dots$ , we compute approximations of  $p(\xi_i^*)$ ,  $p(\xi_j^*)$ ,  $p'(\xi_i^*)$ , and  $p'(\xi_j^*)$  to  $L$  bits after the binary point; see Footnote 6. We stop doubling  $L$  for a particular pair  $(i, j)$  if we can either verify that

$$|v_i|, |v_j| > w(I) \quad \text{or} \quad |v_i - v_j| < \frac{w(I)}{4n} \quad (3.3)$$

or that

$$|v_i|, |v_j| < 2 \cdot w(I) \quad \text{and} \quad |v_i - v_j| > \frac{w(I)}{8n}. \quad (3.4)$$

If (3.3) holds, we discard the pair  $(i, j)$ . Otherwise, we compute sufficiently good approximations (see Footnote 6) of the values  $p(\xi_i^*)$ ,  $p(\xi_j^*)$ ,  $p'(\xi_i^*)$ , and  $p'(\xi_j^*)$ , such that we can derive an approximation  $\tilde{\lambda}_{i,j}$  of

$$\lambda_{i,j} := \xi_i^* + \frac{\xi_j^* - \xi_i^*}{v_j - v_i} \cdot v_i \quad (3.5)$$

with  $|\tilde{\lambda}_{i,j} - \lambda_{i,j}| \leq \frac{1}{32N_I}$ . If  $\tilde{\lambda}_{i,j} \notin [a, b]$ , we discard the pair  $(i, j)$ .

Otherwise, let  $\ell_{i,j} := \lfloor \frac{4N_I(\tilde{\lambda}_{i,j} - a)}{w(I)} \rfloor$ . Then, it holds that  $\ell_{i,j} \in \{0, \dots, 4N_I\}$ . We further define

$$\begin{aligned} I_{i,j} &:= (a_{i,j}, b_{i,j}) \\ &:= \left( a + \max(0, \ell_{i,j} - 1) \cdot \frac{w(I)}{4N_I}, a + \min(4N_I, \ell_{i,j} + 2) \cdot \frac{w(I)}{4N_I} \right). \end{aligned}$$

If  $a_{i,j} = a$ , we set  $a_{i,j}^* := a$ , and if  $b_{i,j} = b$ , we set  $b_{i,j}^* := b$ . For all other values for  $a_{i,j}$  and  $b_{i,j}$ , we choose arbitrary points (see Footnote 6)

$$a_{i,j}^* \in a_{i,j}[\varepsilon \cdot \frac{w(I)}{N_I}] \quad \text{and} \quad b_{i,j}^* \in b_{i,j}[\varepsilon \cdot \frac{w(I)}{N_I}]. \quad (3.6)$$

<sup>6</sup>In order to distinguish the tests from their counterparts in [21], we use the affix `_signat`, which refers to the sign evaluation of  $p$  at the endpoints of an interval  $I$  in order to test  $I$  for the existence of a root. We also remark that we directly give both tests in its full generality. That is, at several places, we use approximate arithmetic, and, in addition, we allow to choose an arbitrary point  $m_i$  from  $m[\delta]$ , where  $m[\delta] := \{m_i := m + (i - \lfloor k/2 \rfloor) \cdot \delta; i = 0, \dots, 2 \cdot \lfloor k/2 \rfloor\}$  is a set of  $2 \cdot \lfloor k/2 \rfloor + 1$  points that are clustered at  $m$ . For now, the reader may assume that we always choose  $m_i = m$ , and that exact arithmetic over rational numbers is used. However, for our variant of the root isolation algorithm that uses approximate arithmetic (see Section 4), we will exploit the fact that we can choose a point  $m_i$  from  $m[\delta]$  for which  $|p(m_i)|$  becomes large. This guarantees that the precision does not become unnecessarily large.

We define  $I' := I_{i,j}^* := (a_{i,j}^*, b_{i,j}^*)$ . Notice that  $I'$  is contained in  $I$ , and it holds that  $\frac{w(I)}{8N_I} \leq w(I') \leq \frac{w(I)}{N_I}$ . In addition, if the endpoints of  $I$  are dyadic, then the endpoints of  $I'$  are dyadic as well.

In the final step, we compute the sign of  $p(a_{i,j}^*)$  and  $p(b_{i,j}^*)$ .  $I'$  is isolating for  $\xi$  if and only if  $p(a_{i,j}^*) \cdot p(b_{i,j}^*) < 0$ , hence, if the latter inequality is fulfilled, we return  $I'$ . Otherwise, we discard  $(i, j)$ .

We say that the `Newton-Test_signat` succeeds if it returns an interval  $I' = I_{i,j}^*$  for at least one of the three pairs  $(i, j)$ . If we obtain an interval for more than one pair, we can output either one of them. Otherwise, the test fails.

If the `Newton-Test_signat` succeeds, we replace  $\mathcal{A} = (I, N_I)$  by  $\mathcal{A} := (I', N_{I'})$ , with  $N_{I'} := N_I^2$ . If the `Newton-Test_signat` fails, we continue with the so-called `Boundary-Test_signat`. Essentially, it checks whether  $\xi$  is located very close to one of the endpoints of  $I$ .

**Boundary-Test\_signat:** Let  $m_\ell := a + \frac{w(I)}{2N_I}$  and  $m_r := b - \frac{w(I)}{2N_I}$ , and let  $\varepsilon := 2^{-\lceil 2 + \log n \rceil}$ . Choose arbitrary points (see Footnote 6)

$$m_\ell^* \in m_\ell[\varepsilon \cdot \frac{w(I)}{N_I}] \quad \text{and} \quad m_r^* \in m_r[\varepsilon \cdot \frac{w(I)}{N_I}], \quad (3.7)$$

and compute the sign of  $p(x)$  at  $x = a$ ,  $x = m_\ell^*$ ,  $x = m_r^*$ , and  $x = b$ . If  $p(a) \cdot p(m_\ell^*) < 0$ , then  $I' := (a, m_\ell^*)$  isolates  $\xi$ , and thus, we return  $I'$ . If  $p(b) \cdot p(m_r^*) < 0$ , we return  $I' = (m_r^*, b)$ . Notice that from our definition of  $m_\ell^*$  and  $m_r^*$ , it follows that both intervals  $I_\ell$  and  $I_r$  have width in between  $\frac{w(I)}{4N_I}$  and  $\frac{w(I)}{N_I}$ . If  $p(a) \cdot p(m_\ell^*) < 0$  or  $p(b) \cdot p(m_r^*) < 0$ , the `Newton-Test_signat` succeeds. Otherwise, the test fails.

If the `Boundary-Test_signat` succeeds, then  $\mathcal{A} = (I, N_I)$  is replaced by  $\mathcal{A} := (I', N_{I'})$ , with  $N_{I'} := N_I^2$ . If the `Newton-Test_signat` as well as the `Boundary-Test_signat` fail, then we choose an arbitrary point (see Footnote 6)

$$m^* \in m(I) \left[ \frac{w(I)}{2^{\lceil 2 + \log n \rceil}} \right] \quad (3.8)$$

and compute the sign of  $p(x)$  at  $x = a$  and  $x = m^*$ . If  $p(a) \cdot p(m^*) < 0$ , we replace  $\mathcal{A} = (I, N_I)$  by  $\mathcal{A} := (I', N_{I'})$ , with  $I' = (a, m^*)$  and  $N_{I'} := \max(4, \sqrt{N_I})$ . If  $p(m^*) = 0$ , we stop and return the interval  $[m^*]$  of width zero. Otherwise, we replace  $\mathcal{A} = (I, N_I)$  by  $\mathcal{A} := (I', N_{I'})$ , with  $I' = (m^*, b)$  and  $N_{I'} := \max(4, \sqrt{N_I})$ . We stop refining  $I$  as soon as  $I$  has width less than  $2^{-L}$ .

We formulated the `Newton-Test_signat` and the `Boundary-Test_signat` in a way such that each of them succeeds if the corresponding test in [21] succeeds, assuming that we choose the same points in (3.2), (3.6), and in (3.7). Namely, if  $I' = (a', b')$  is known to contain at most one (simple) root of  $p$ , then  $\text{var}(p, I') = 0$  implies that  $p(a') \cdot p(b') \geq 0$ .<sup>7</sup> Hence, the analysis from [21] directly carries over and yields the following result:<sup>8</sup>

**LEMMA 6.** *Let  $I_0, I_1, \dots, I_s$ , with  $I_0 \supset I_1 \supset \dots \supset I_s$ ,  $s \in \mathbb{N}$ , and  $w(I_{s-1}) \geq 2^{-L} > w(I_s)$ , be the intervals produced by the algorithm `NEWREFINE`, and let  $s_{\max}$  be the largest number of intervals  $I_j$  for which the one-circle region of  $I_j$  contains exactly the same roots. Then, it holds that  $s_{\max} = O(\log n + \log(\tau + L))$ .*

<sup>7</sup>  $p(a') \cdot p(b') \geq 0$  implies that  $I'$  contains no root but not that  $\text{var}(p, I') = 0$ .

<sup>8</sup> The proof of Lemma 6 is essentially identical to our considerations in [21, Section 3.2 and 4.1]. In particular, the proofs of [21, Lemma 20 and 23] directly carry over if we use that  $\log N_I$  is always bounded by  $O(\tau + L)$  when refining  $I_0$  to a width less than  $2^{-L}$ .

From the lemma above and Theorem 5, we now obtain the following bound for the number of iterations that is needed to refine  $I_0$  to an interval of width less than  $2^{-L}$ .

**THEOREM 7.** *Let  $I_0 = (a_0, b_0) \subset (0, 2^{\tau+1})$ , with  $a_0, b_0 \in \mathbb{Q}$ , be an isolating interval for a simple root  $\xi$  of a  $k$ -nomial  $p \in \mathbb{Z}[x]$  of magnitude  $(n, \tau)$ . For computing an interval  $I = (a, b) \subset I_0$ , with  $a, b \in \mathbb{Q}$  and  $\xi \in I$ , the algorithm `NEWREFINE` needs  $O(\text{var}(p, I_0) \cdot (\log n + \log(\tau + L)))$  many iterations and  $O(k \cdot \log n \cdot \text{var}(p, I_0) \cdot (\log n + \log(\tau + L)))$  many arithmetic operations over  $\mathbb{Q}$ .*

**PROOF.** As in Lemma 6, we denote  $I_0, I_1, \dots, I_s$ , with  $I_0 \supset I_1 \supset \dots \supset I_s$ ,  $s \in \mathbb{N}$ , and  $w(I_{s-1}) \geq 2^{-L} > w(I_s)$ , the intervals produced by `NEWREFINE`. Let  $j_0$  be the minimal index  $j$  for which the one-circle region  $A_0$  of  $I_j$  contains at most  $v_0$  many roots, with  $v_0 := \text{var}(p, I_0)$ . If the one-circle region of each  $I_j$  contains more than  $v_0$  roots, we set  $j_0 := s$ . Now, using Lemma 6 for the sub-sequence  $I_{j_0}, \dots, I_s$ , we conclude that  $s - j_0 = v_0 \cdot s_{\max}$ . Hence, we are left to argue that  $j_0$  is bounded by  $O(v_0 \cdot (\log n + \log(\tau + L)))$ . In fact, the following consideration even shows that  $j_0 = O(\log n + \log(\tau + L))$ : We first consider the special case, where  $I_{j_0}$  shares a common endpoint with  $I_0$ . Then, exactly the same argument as in the proof of [21, Lemma 23] shows that  $j_0$  is bounded by  $O(\log n + \log(\tau + L))$ , where we use that  $N_{I_j} = O(L + \tau)$  for all  $j$ . Essentially, this is due to the fact that success of the `Boundary-Test_signat` guarantees quadratic convergence, and the latter test must succeed for all but  $O(\log n + \log(\tau + L))$  many iterations. Now suppose that there exists an index  $j'_0 < j_0$  such that  $I_{j'_0}$  shares a common endpoint with  $I_0$ , whereas  $I_{j'_0+1}$  does not. Then,  $j'_0 = O(\log n + \log(\tau + L))$ . In addition, the distance from any point  $x \in I_{j'_0+1}$  to each of the two endpoints  $a_0$  and  $b_0$  is larger than or equal to  $w(I_{j'_0+1})/4$ . Hence, since  $w(I_{j+1}) \leq \frac{3}{4} \cdot w(I_j)$  for all  $j$ , we have  $\max(|a_j - a_0|, |b_j - b_0|) > 8n^2 \cdot w(I_j)$  for all  $j > j'_0 + 4(\log n + 1)$ . According to [20, Lemma 9], it follows that the one-circle region of any interval  $I_j$ , with  $j > j'_0 + 4(\log n + 1)$ , is contained in the Obreshkoff lens  $L_n$  of  $I_0$ . Now, from part (a) of Lemma 5, we conclude that the one-circle region of  $I_j$  contains at most  $v_0$  roots for each  $j > j'_0 + 4(\log n + 1)$ , and thus,  $j_0 = O(\log n + \log(\tau + L))$ . This proves the first claim.

For the second claim, we remark that, in each iteration, we perform a constant number of evaluations of the polynomial  $p$  and its derivative  $p'$ . Since both polynomials have  $k$  coefficients or less, this shows that we need  $O(k \log n)$  arithmetic operations over  $\mathbb{Q}$  in each iteration. Multiplication of the latter bound with the bound on the number of iterations eventually yields the claimed bound on the arithmetic complexity.  $\square$

Now suppose that isolating intervals  $I_1, \dots, I_{k_0} \subset \mathcal{I}$  for all simple real roots of  $p$  are given. Then,  $\sum_{j=1}^{k_0} \text{var}(p, I_j) \leq \text{var}(p, \mathcal{I}) \leq k$ , and thus, Theorem 7 yields the following result:

**COROLLARY 8.** *Let  $p \in \mathbb{Z}[x]$  be a  $k$ -nomial of magnitude  $(n, \tau)$ , and  $I_j = (a_j, b_j) \subset \mathcal{I} = (0, 2^{\tau+1})$ , with  $j = 1, \dots, k_0$  and  $a_j, b_j \in \mathbb{Q}$ , be isolating intervals for all simple real roots of  $p$ . Then, we can refine all intervals  $I_j$  to a width less than  $2^{-L}$ , with  $L$  an arbitrary positive integer, with a number of arithmetic operations over  $\mathbb{Q}$  bounded by  $O(k^2 \cdot \log n \cdot (\log n + \log(\tau + L)))$ .*

## 4. BIT COMPLEXITY

We finally aim to derive a bound on the bit complexity of our algorithm when using approximate but certified arithmetic. When using exact arithmetic over dyadic numbers (i.e. numbers of the form  $m \cdot 2^{-l}$ , with  $m, l \in \mathbb{Z}$ ), all intermediate results are dyadic and of bit-size  $O(n^2(\log n + \tau))$ . Namely, we refine intervals to a width of

size  $2^{-O(n(\tau+\log n))}$ , and only consider evaluations of the polynomial  $p$  at dyadic points that are contained in such intervals and whose bit-size is bounded by  $\kappa = O(n(\tau + \log n))$ . From the latter fact and Theorem 3, we conclude that the overall bit complexity of our algorithm is bounded by  $\tilde{O}(n^2 \tau \cdot k^3)$  when using exact arithmetic over rational (dyadic) numbers. Here, we use that exact evaluation of  $p$  at a dyadic number of bit-size  $\kappa$  needs  $\tilde{O}(n(\kappa + \tau))$  bit operations [2, Lemma 2]. However, the following considerations show that we can replace a factor  $n$  by an additional factor  $k$  in the latter bound. More precisely, using approximate computation, we can reduce the bit-size of the intermediate results by a factor  $n$  for the price of using  $k$  times as many arithmetic operations. We give details:

Notice that, at several places in the algorithm NEWREFINE, that is, in (3.2), (3.6), (3.7), and in (3.8), we are free to choose an arbitrary point  $m_i$  from a set

$$m[\delta] := \{m_i := m + (i - \lceil k/2 \rceil) \cdot \delta; i = 0, \dots, 2 \cdot \lceil k/2 \rceil\}$$

consisting of  $\lceil k/2 \rceil + 1$  points that are clustered at  $m$ . Now, in order to keep the precision of the computations as low as possible, we aim to choose a point  $m_i \in m[\delta]$  for which  $p(m_i)$  has a large absolute value. We introduce the following definition that has already been used in [21, Section 2.2] in a slightly modified form.

**DEFINITION 1.** For  $m[\delta]$  as above, we call a point  $m^* \in m[\delta]$  admissible with respect to  $m[\delta]$  (or just admissible if there is no ambiguity) if  $|p(m^*)| \geq \frac{1}{4} \cdot \max_i |p(m_i)|$ .

**LEMMA 9.** Suppose that each point in  $m[\delta]$  has absolute value less than  $2^{\tau+1}$  and that  $\lambda := \max_i |p(x_i)| \neq 0$ . Then, we can determine an admissible point  $m^* \in m[\delta]$  and an integer  $t$  with

$$2^{t-1} \leq |p(m^*)| \leq \lambda \leq 2^{t+1}$$

with  $\tilde{O}(k(n\tau + \log \max(\lambda^{-1}, 1)))$  many bit operations.

**PROOF.** Using the same approach as in [11, Section 4] plus repeated squaring, we can evaluate  $p$  at any of the  $\lceil k/2 \rceil + 1$  many points  $x = m_i$  to an absolute error less than  $2^{-K}$ , with  $K$  an arbitrary positive integer, in a number of bit operations bounded by  $\tilde{O}(k \cdot (n\tau + K))$ . We can now compute an admissible point  $m^* \in m[\delta]$  as follows: Consider  $K = 1, 2, 4, 8, \dots$  and approximate all values  $|p(m_i)|$  to a precision of  $K$  bits after the binary point until, for at least one  $i$ , we obtain an approximation  $2^{t_i}$  with  $t_i \in \mathbb{Z}$  and  $2^{t_i-1} \leq |p(x_i)| \leq 2^{t_i+1}$ . Now, let  $t_0$  be such that  $t_{i_0}$  is maximal; then, it follows that  $2^{t_0-1} \leq \lambda \leq 2^{t_0+1}$ . Following this approach, we must stop for a  $K$  with  $K < 2 \log \max(\lambda^{-1}, 1)$ . Since we double  $K$  at most  $\log \log \max(\lambda^{-1}, 1)$  many times, the claim follows.  $\square$

Now, in (3.2), (3.6), (3.7), and in (3.8) of NEWREFINE, we do not choose an arbitrary point from the corresponding set  $m[\delta]$  but an admissible point  $m^* \in m[\delta]$ . We argue that, for each such  $m^*$ , we have  $|p(m^*)| > 2^{-O(n(\tau+\log n))}$ : Let  $I = (a, b)$  be the interval that is processed in the current iteration, then  $\min(|m^* - a|, |m^* - b|) > n\delta \geq (\sin \frac{\pi}{2n+2})^{-1} \cdot \frac{\delta}{2}$ . Hence, the distance from  $m^*$  to the boundary of the Obreshkoff lens  $L_n$  of  $I$  is larger than  $\delta/2$  since the distance from an arbitrary point  $x \in I = (a, b)$  to the boundary of  $L_n$  is larger than  $\min(|x - a|, |x - b|) \cdot \sin \frac{\pi}{2n+2}$ ; see [20, Lemma 5 and Figure 4.1]. Since the Obreshkoff lens  $L_n$  of the larger interval  $I_0$  contains at most  $k$  roots (counted with multiplicity), it follows that there exists at least one point  $m_{i_0} \in m[\delta]$  with  $|\xi_j - m_{i_0}| \geq \delta/2$  for all (distinct) complex roots  $\xi_j$  of  $p$ . Let  $\xi_{j_0}$  be the root of  $p$  that minimizes the distance to  $m_{i_0}$ . If  $\xi_{j_0} = \xi$ , then

$$\frac{|p(m_{i_0})|}{|p'(\xi)|} = |m_{i_0} - \xi| \cdot \prod_{i \neq j_0} \left( \frac{|m_{i_0} - \xi_i|}{|\xi - \xi_i|} \right)^{\mu_j} \geq |m_{i_0} - \xi| \cdot 2^{-n+1} \geq \frac{\delta}{2^n},$$

where  $\mu_j$  denotes the multiplicity of  $\xi_j$  as a root of  $p$ . Hence, from  $\delta \geq 2^{-\lceil 5+\log n \rceil} \cdot \frac{w(I)}{N_I} = 2^{-O(\log n + \tau + L)}$ , we conclude that  $|p(m_{i_0})| = 2^{-O(n(\log n + \tau))}$  if  $w(I) \geq 2^{-L}$ , with  $L := 128n \cdot (\log n + \tau)$ . We are left to discuss the case  $\xi_{j_0} \neq \xi$ . Then,

$$\begin{aligned} \frac{|p(m_{i_0})|}{|p^{(\mu_{j_0})}(\xi_{j_0})|} &= |m_{i_0} - \xi_{j_0}|^{\mu_{j_0}} \cdot \prod_{i \neq j_0} \left( \frac{|m_{i_0} - \xi_i|}{|\xi_{j_0} - \xi_i|} \right)^{\mu_j} \geq \frac{|m_{i_0} - \xi_{j_0}|^{\mu_{j_0}}}{2^{n-1}} \\ &\geq 2^{-2n} \cdot \delta^{\mu_{j_0}} \geq 2^{-2n - n(6 + \log n)} \cdot \left( \frac{w(I)}{N_I} \right)^{\mu_{j_0}}. \end{aligned}$$

Trivially, we have  $w(I) \leq 2 \cdot w(I)/\sqrt{N_I}$  for  $N_I = 4$ . If  $N_I > 4$ , then there must have been an iteration, where we replaced an isolating interval  $J$  for  $\xi$ , with  $I \subset J \subset (0, 2^{\tau+1})$  by an interval  $J'$ , with  $I \subset J' \subset J$  and  $w(J') \leq w(J)/\sqrt{N_I}$ . Hence, in any case, we have  $w(I) \leq 2^{\tau+2}/\sqrt{N_I}$ . This shows that

$$\left( \frac{w(I)}{N_I} \right)^{\mu_{j_0}} \geq w(I)^{3\mu_{j_0}} \cdot 2^{-2\mu_{j_0} \cdot (\tau+2)} \geq |\xi - \xi_{j_0}|^{3\mu_{j_0}} \cdot 2^{-2n(\tau+2)},$$

where the second to last inequality follows from the inequality  $|\xi - \xi_{j_0}| \leq |\xi - m_{i_0}| + |m_{i_0} - \xi_{j_0}| \leq w(I) + |m_{i_0} - \xi_{j_0}|$ . Then, Theorem 2 (with  $F := p \cdot 1$ ) implies that  $\left( \frac{w(I)}{N_I} \right)^{\mu_{j_0}} = 2^{-O(n(\log n + \tau))}$ . In summary, we conclude that, in (3.2), (3.6), (3.7), and in (3.8), we can choose points  $m_i \in m[\delta]$  with  $|p(m_i)| = 2^{-O(n(\log n + \tau))}$  for the cost of  $\tilde{O}(k \cdot n\tau)$  bit operations. Notice that, for the same cost, we can also determine the sign of  $p$  at each of these points, and thus, the considered sign evaluations in one iteration need  $\tilde{O}(k \cdot n\tau)$  bit operations.

It remains to bound the cost for computing the approximations  $\tilde{\lambda}_{j_1, j_2}$  as defined in (3.5) in NEWREFINE. Notice that, for checking the inequalities in (3.3) and in (3.4), it suffices to approximate the values  $p(\xi_{j_1}^*)$ ,  $p(\xi_{j_2}^*)$ ,  $p'(\xi_{j_1}^*)$ , and  $p'(\xi_{j_2}^*)$  to an absolute error of

$$\log \min(p(\xi_{j_1}^*), p(\xi_{j_2}^*)) + O(\log(n/w(I))) = O(n(\log n + \tau))$$

bits after the binary point. Again, the cost for computing such approximations is bounded by  $\tilde{O}(k \cdot n\tau)$  bit operations. Then, the same complexity bounds also holds for the computation of  $\tilde{\lambda}_{j_1, j_2}$ . Namely, since  $v_{j_1} - v_{j_2}$  has absolute value larger than  $w(I)/(8n)$ , and  $v_{j_1}$  as well as  $v_{j_2}$  have absolute value smaller than  $2^{O(n\tau)}$ , it suffices to carry out all operations with a precision of  $O(\log N_I + \log w(I)^{-1} + n\tau)$  bits after the binary point. We summarize:

**LEMMA 10.** Let  $p \in \mathbb{Z}[x]$  be a  $k$ -nomial of magnitude  $(n, \tau)$ , and let  $I_j = (a_j, b_j) \subset \mathcal{I} = 2^{\tau+1}$ , with  $j = 1, \dots, k_0$ , be isolating intervals for all simple real roots of  $p$ . Suppose that  $a_j, b_j \in \mathbb{Q}$  and  $\min_j \min(|p(a_j)|, |p(b_j)|) > 2^{-L}$ , with  $L := 128n \cdot (\log n + \tau)$ . Then, NEWREFINE refines all intervals  $I_j$  to a width less than  $2^{-L}$  with a number of bit operations bounded by  $\tilde{O}(k^3 \cdot n\tau)$ . For each interval  $I'_j = (a'_j, b'_j)$  returned by NEWREFINE, we have  $a'_j, b'_j \in \mathbb{Q}$  and  $\min(|p(a'_j)|, |p(b'_j)|) > 2^{-L}$ .

**PROOF.** The result is an almost immediate consequence of our considerations above. Notice that the condition on the endpoints of the initial intervals  $I_j$  guarantees that we only evaluate the sign of  $p$  at points that are either admissible points  $m^* \in m[\delta]$  or endpoints of one of the intervals  $I_j$ . Hence, each such sign evaluation needs  $\tilde{O}(k \cdot n\tau)$  bit operation. For the computation of an admissible point, we need  $\tilde{O}(k^2 \cdot n\tau)$  many bit operations, which is due to the fact that we perform approximate computation of  $p$  at  $O(k)$  many points in parallel. From Theorem 7, we conclude that the number of iterations in total is bounded by  $O(k \cdot \log(n\tau))$ , and thus, the claimed bound on the bit complexity follows.  $\square$

For our root isolation algorithm as proposed in Section 2.1, the above result implies that we can isolate all real roots of  $p$  with a number of bit operations bounded by  $\tilde{O}(k^4 \cdot n(\tau + k))$ . Namely, in each step of the recursion, we first have to evaluate some  $k$ -nomial  $p_{j-1}$  of magnitude  $(n, \tau + k \log n)$  at arbitrary points  $x_i \in I_{j,i}$ , where  $I_{j,i} = (a_{j,i}, b_{j,i})$  are isolating intervals for the real roots of  $p_j$ . Since it suffices to compute approximations of the values  $p_{j-1}(x_i)$  to  $L/2$  bits after the binary point, the cost for all evaluations is bounded by  $\tilde{O}(k^2 \cdot n\tau)$  bit operations. In a second step, we have to refine all isolating intervals  $I'_{j,i}$  for the simple real roots of  $p_j$  to a width less than  $2^{-L}$ , with  $L = 128n(\log n + \tau)$ . Each endpoint  $e$  of an arbitrary  $I_{j,i}$  is an endpoint of one of the intervals  $I_{j,i}$ , that is,  $e = a_{j,i}$  or  $e = b_{j,i}$  for some  $i$ . Hence, by induction, it follows that  $p(e) \geq 2^{-L}$ . Then, from Lemma 10, we conclude that refining all intervals to a width less than  $2^{-L}$  needs  $\tilde{O}(k^4 \cdot n(\tau + k))$  bit operations.

**THEOREM 11.** *Let  $p \in \mathbb{Z}[x]$  be a  $k$ -nomial of magnitude  $(n, \tau)$ . Then, computing isolating intervals with rational endpoints for all real roots of  $p$  needs  $\tilde{O}(k^3 \cdot n\tau)$  bit operations. For  $k = O(\log(n\tau)^C)$ , with  $C$  a fixed positive constant, the latter bound becomes  $\tilde{O}(n\tau)$ , which is optimal up to logarithmic factors.*

**PROOF.** It remains to prove the last claim. For this, consider the polynomial  $p(x) = x^n - (2^{2^\tau} \cdot x^2 - a)^2$ , where  $a > 1$  is a fixed constant integer, and  $n, \tau \in \mathbb{N}_{\geq 8}$ . Then,  $p$  is a 4-nomial of magnitude  $(n, O(\tau))$ , and  $p$  has two positive roots  $x_1$  and  $x_2$ , with  $x_1 < x_2$  and  $|x_i - \sqrt{a} \cdot 2^{-\tau}| < 2^{-\Omega(n\tau)}$  for  $i = 1, 2$ . Namely, let  $f(x) := (2^{2^\tau} \cdot x^2 - a)^2$  be a polynomial that has two roots of multiplicity 2 at  $x = \pm \sqrt{a} \cdot 2^{-\tau}$ , and let  $g(x) := x^n$ . Then, a simple computation shows that  $|f(z)| > |g(z)|$  for all points  $z$  on the boundary of the disk  $\Delta \subset \mathbb{C}$  of radius  $\varepsilon := 2^{-(n-2)(\tau-2)} \cdot a^{n/2-1}$  centered at  $\sqrt{a} \cdot 2^{-\tau}$ . Hence, Rouché's Theorem implies that  $f$  and  $p = g - f$  have the same number of roots in  $\Delta$ . In addition, both roots are real.

We conclude that, for any isolating interval  $I_1 = (a_1, b_1)$  for  $x_1$ , we must have  $|b_1 - \sqrt{a} \cdot 2^{-\tau}| < 2^{-\Omega(n\tau)}$ . Now, let  $b_1 = p/q$  with coprime integers  $p$  and  $q$ , then we must have  $q = \Omega(n\tau)$ ; see Lemma 13 in the Appendix. Hence, the binary representation of the endpoints of  $I_1$  already needs  $\Omega(n\tau)$  bits, which proves our claim.  $\square$

## 5. CONCLUSION

In this paper, we give the first algorithm that computes the real roots of a sparse polynomial  $p \in \mathbb{Z}[x]$  in a number of arithmetic operations over  $\mathbb{Q}$  that is polynomial in the input size of the sparse representation of  $p$ . In addition, for sparse-enough polynomials, the algorithm achieves a near-optimal bound for the bit complexity of the problem of isolating all real roots. The main ingredients of our algorithm are evaluation and separation bounds as well as an efficient method for refining an isolating interval of a simple real root. So far, our algorithm has been formulated in the easiest possible way with the prior goal to achieve good theoretical complexity bounds, however, for the price of a probably worse efficiency in practice. Hence, our first research goal is to provide an efficient implementation of our algorithm that integrates additional steps in order to improve its practical efficiency. Our second research goal is to extend our algorithm to (square-free) polynomials with arbitrary real coefficients. For this, it seems reasonable to combine our algorithm with the root isolation method from [21]. Hopefully, this allows us to derive improved (bit) complexity bounds for sparse polynomials that can be stated in terms of the geometry of the roots (similar to the bounds as provided in [21, Theorem 31] or [14, Theorem 3]) rather than in terms of the input size. For polynomials  $p \in \mathbb{R}[x]$  that may have multiple real roots, the situation becomes more complicated. Namely, since no a-priori separation bound is

known to decide whether a certain root has multiplicity larger than one, we cannot distinguish between a real root of multiplicity  $m > 1$  and a cluster of  $m$  (not necessarily real) roots. Hence, it remains an open research question whether the computation of a (reasonable good) separation bound has polynomial arithmetic complexity.

## 6. REFERENCES

- [1] O. Bastani, C. J. Hillar, D. Popov, and J. M. Rojas. Randomization, Sums of Squares, Near-Circuits, and Faster Real Root Counting. *Contemporary Mathematics*, 556:145–166, 2011.
- [2] Y. Bouzidi, S. Lazard, M. Pouget, and F. Rouillier. Rational univariate representations of bivariate systems and applications. In *ISSAC*, pages 109–116, 2013.
- [3] M. Burr and F. Krahmer. SqFreeEVAL: An (almost) optimal real-root isolation algorithm. *J. Symb. Comput.*, 47(2):153–166, 2012.
- [4] J. Cohn. The length of the period of the simple continued fraction of  $\sqrt{d}$ . *Pacific Journal of Mathematics*, 71(1):21–32, 1977.
- [5] G. E. Collins and A. G. Akritas. Polynomial real root isolation using Descartes' rule of signs. In R. D. Jenks, editor, *SYMSAC*, pages 272–275, Yorktown Heights, NY, 1976. ACM Press.
- [6] F. Cucker, P. Koiran, and S. Smale. A polynomial time algorithm for diophantine equations in one variable. *J. Symb. Comput.*, 27(1):21–29, 1999.
- [7] A. Eigenwillig. *Real Root Isolation for Exact and Approximate Polynomials Using Descartes' Rule of Signs*. PhD thesis, Saarland University, Germany, 2008.
- [8] A. Eigenwillig, V. Sharma, and C.-K. Yap. Almost tight complexity bounds for the Descartes method. In *ISSAC*, pages 151–158, 2006.
- [9] M. E. A. Garcia and A. Galligo. A root isolation algorithm for sparse univariate polynomials. In *ISSAC*, pages 35–42, 2012.
- [10] H. W. L. (Jr.). Finding small degree factors of lacunary polynomials. *Number Theory in Progress*, 1:267–276, 1999.
- [11] M. Kerber and M. Sagraloff. Efficient Real Root Approximation. In *ISSAC*, pages 209–216, 2011.
- [12] S. Lang. *Introduction to Diophantine Approximations*. Springer books on elementary mathematics. Springer, 1995.
- [13] J. McNamee. *Numerical Methods for Roots of Polynomials*. Number 2 in Studies in Computational Mathematics. Elsevier Science, 2013.
- [14] K. Mehlhorn, M. Sagraloff, and P. Wang. From Approximate Factorization to Root Isolation with Application to Cylindrical Algebraic Decomposition. *CoRR*, abs/1301.4870, 2013. a preliminary version appeared in *ISSAC*, pages 283–290, 2013.
- [15] N. Obreshkoff. *Verteilung und Berechnung der Nullstellen reeller Polynome*. VEB Deutscher Verlag der Wissenschaften, 1963.
- [16] N. Obreshkoff. *Zeros of Polynomials*. Marina Drinov, Sofia, 2003. Translation of the Bulgarian original.
- [17] V. Pan. Univariate Polynomials: Nearly Optimal Algorithms for Numerical Factorization and Root Finding. *J. Symb. Comput.*, 33(5):701–733, 2002.
- [18] J. M. Rojas and Y. Ye. On solving univariate sparse polynomials in logarithmic time. *J. Complexity*, 21(1):87–110, 2005.
- [19] F. Rouillier and P. Zimmermann. Efficient isolation of [a] polynomial's real roots. *J. Computational and Applied Mathematics*, 162:33–50, 2004.
- [20] M. Sagraloff. When Newton meets Descartes: a simple and fast algorithm to isolate the real roots of a polynomial. In *ISSAC*, pages 297–304, 2012.
- [21] M. Sagraloff and K. Mehlhorn. Computing real roots of real polynomials - an efficient method based on Descartes' Rule of Signs and Newton iteration. *CoRR*, abs/1308.4088, 2013.
- [22] M. Sagraloff and C.-K. Yap. A simple but exact and efficient algorithm for complex root isolation. In *ISSAC*, pages 353–360, 2011.
- [23] A. Schönhage. The Fundamental Theorem of Algebra in Terms of Computational Complexity. Technical report, Math. Inst. Univ. Tübingen, 1982.
- [24] E. P. Tsigaridas. Improved bounds for the CF algorithm. *Theor. Comput. Sci.*, 479:120–126, 2013.
- [25] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, 1999.



## 7. APPENDIX

**THEOREM 12.** *Let  $f$  and  $g$  be polynomials of degree  $n$  or less with integer coefficients of absolute values less than  $2^\mu$ , and let*

$$L := 128 \cdot n \cdot (\log n + \mu). \quad (7.1)$$

*Then, for any two distinct roots  $\xi_i$  and  $\xi_j$  of  $F := f \cdot g$ , it holds that  $|\xi_i - \xi_j|^{m_i} > 2^{-L}$ , where  $m_i := \text{mult}(\xi_i, F)$  denotes the multiplicity of  $\xi_i$  as a root of  $F$ . If  $\xi$  is a root of  $g$  and  $f(\xi) \neq 0$ , then it holds that  $|f(x)| > 2^{-L/4}$  for all  $x \in \mathbb{C}$  with  $|x - \xi| < 2^{-L}$ . Vice versa, if  $f(\xi) = 0$ , then  $|f(x)| < 2^{-L}$  for all  $x \in \mathbb{C}$  with  $|x - \xi| < 2^{-L}$ .*

**PROOF.** For the proof, we mainly combine known results [14], however, we aim to stress the fact that the following computations are necessary to derive an  $L$  of size  $O(n(\log n + \tau))$ . Namely, the literature only provides comparable bounds for square-free polynomials, whereas, for arbitrary polynomials, the existing bounds are of size  $\tilde{O}(n^2 + n\mu)$ . This is mainly due to the fact that the known bounds for square-free polynomials are directly applied to the square-free part, and, in general, the square-free part of an integer polynomial of magnitude  $(n, \mu)$  is of magnitude  $(n, O(n + \mu))$ .

Let  $F(x) = f(x) \cdot g(x) = F_N \cdot \prod_{j=1}^N (x - z_j)$ , where  $z_1, \dots, z_N$  denote the complex roots of  $F$ . Then,  $F$  has degree  $N \leq 2n$  and its coefficients are integers of absolute value  $2^{\tau_F}$  with  $\tau_F < 2(\mu + \log n)$ . Now, suppose that  $F$  has exactly  $r_0$ , with  $1 \leq r_0 \leq \deg F$ , distinct complex roots  $\xi_1$  to  $\xi_{r_0}$  with multiplicities  $m_1$  to  $m_{r_0}$ , respectively. From the proof of [14, Theorem 5], we conclude that

$$\prod_{i=1}^{r_0} \min \left( 1, \frac{|F^{(m_i)}(\xi_i)|}{|F_N| \cdot m_i!} \right) \geq \left( 2^{3\tau_F + 2 \cdot \log N + 1} \cdot \text{Mea}(F) \right)^{-N},$$

where  $\text{Mea}(F) = |F_N| \cdot \prod_{i=1}^{r_0} \max(1, |\xi_i|)^{m_i}$  denotes the Mahler Measure of  $F$  and  $F^{(m)}(x) := \frac{d^m F(x)}{dx^m}$  the  $m$ -th derivative of  $F$ . Since  $\text{Mea}(F) \leq \|F\|_2 \leq \sqrt{N+1} \cdot 2^{\tau_F}$ , a simple computation shows that

$$\prod_{i=1}^{r_0} \min \left( 1, \frac{|F^{(m_i)}(\xi_i)|}{|F_N| \cdot m_i!} \right) > 2^{-24n(\mu + \log n)}. \quad (7.2)$$

Now, assume that  $\xi = \xi_i$  is a root of  $g$  and that  $f(\xi) \neq 0$ . Then, it follows that

$$|f(\xi)| = \frac{|F^{(m_i)}(\xi_i)|}{|g^{(m_i)}(\xi_i)|} > \frac{2^{-24n(\mu + \log n)}}{(n+1) \cdot 2^\tau \cdot |\xi_i|^n} > 2^{-28n(\mu + \log n)},$$

where we used that  $\xi_i$  is a root of  $g$  of multiplicity  $m_i$  and  $|\xi_i| < 2^{\mu+1}$  for all  $i$ . Hence, if  $w := |x - \xi| < 2^{-L}$ , then

$$\begin{aligned} |f(x)| &= \left| f(\xi) + \frac{f'(\xi)}{1!} \cdot w + \dots + \frac{f^{(n)}(\xi)}{n!} \cdot w^n \right| \\ &\geq |f(\xi)| - w \cdot n^2 \cdot 2^\mu \cdot 2^{n(\mu+1)} \geq 2^{-32(n(\mu + \log n))}. \end{aligned}$$

Vice versa, if we assume that  $f(\xi) = 0$ , then  $|f(x)| < w \cdot n^2 \cdot 2^{n(\mu+1)} < 2^{-64n(\mu + \log n)}$  for all  $x$  with  $|x - \xi| \leq w \leq 2^{-L}$ . This proves the second claim. For the first claim, let  $\xi_i$  and  $\xi_j$  be any two distinct roots of  $F$ . Then, we conclude from (7.2) that

$$\begin{aligned} 2^{-24n(\mu + \log n)} &< \frac{|F^{(m_i)}(\xi_i)|}{|F_N| \cdot m_i!} = \prod_{l \neq i} |\xi_i - \xi_l|^{m_l} \\ &= |\xi_i - \xi_j|^{m_j} \cdot \prod_{l \neq i, j} |\xi_i - \xi_l|^{m_l} \leq |\xi_i - \xi_j|^{m_j} \cdot 2^{2N(\tau_F + 1)}, \end{aligned} \quad (7.3)$$

and thus, the first claim follows.  $\square$

**LEMMA 13.** *Let  $a \in \mathbb{Z}$  be a positive integer such that  $\sqrt{a} \notin \mathbb{Z}$ , and let  $p$  and  $q$  be arbitrary integers. Then,  $|\sqrt{a} - \frac{p}{q}| > \frac{1}{32a^2 \cdot q^2}$ .*

**PROOF.** We consider the continued fraction expansion of  $\sqrt{a}$ :

$$\sqrt{a} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots}}},$$

with non-negative integers  $a_0, a_1, \dots$ . For short, we write  $\sqrt{a} = [a_0; a_1, a_2, \dots]$ . Abbreviating the continued fraction expansion at  $a_n$  yields the corresponding approximation  $\frac{p_n}{q_n} = [a_0; a_1, \dots, a_n]$ , where  $p_n$  and  $q_n$  are co-prime integers. The recursive relation between the denominators  $q_n$  and the values  $a_n$  is given as follows:

$$q_n = a_n \cdot q_{n-1} + q_{n-2}.$$

Furthermore, it holds that the sequence  $(a_1, a_2, \dots)$  is periodic<sup>9</sup>, and each value  $a_i$  is smaller than  $2\sqrt{a}$ ; see [4]. Since the denominators  $q_n$  are monotonously increasing, there exists an  $n_0$  with  $q_{n_0-1} < q \leq q_{n_0}$ . Then, from the above recursion, we conclude that  $q_{n_0} < 2\sqrt{a} \cdot q_{n_0-1} + q_{n_0-2} < 4\sqrt{a} \cdot q$  and  $q_{n_0+1} = a_{n_0+1} \cdot q_{n_0} + q_{n_0-1} < 16 \cdot a \cdot q$ . According to [12, I, §2, Theorem 5], we have

$$\left| \sqrt{a} - \frac{p_n}{q_n} \right| > \frac{1}{2 \cdot q_n \cdot q_{n+1}} \quad \text{for all } n,$$

and thus,

$$\left| \sqrt{a} - \frac{p_{n_0}}{q_{n_0}} \right| > \frac{1}{32a\sqrt{a} \cdot q^2} > \frac{1}{32a^2 \cdot q}.$$

Our claim now follows from the fact that, for all  $n \geq 1$ , the continued fraction approximation  $p_n/q_n$  minimizes the distance between  $\sqrt{a}$  and any rational value  $p/q$  with  $q \leq q_n$ .  $\square$

<sup>9</sup>More precisely, there exists a  $k \in \mathbb{N}$ , with  $k \leq 2a$  such that  $(a_1, a_2, \dots, a_k) = (a_1, a_2, a_3 \dots a_3, a_2, a_1, 2a_0)$  and  $a_{k+i} = a_i$  for all  $i \in \mathbb{N}_{\geq 1}$ .